DEFENSE INTELLIGENCE AGENCY

Department of Defense Intelligence Management System

SECURITY REQUIREMENTS

Prepared for
DoDIMS PMO
National Intelligence Production Center
DIA/PO-5C

Prepared by:
J.G. Van Dyke & Associates, Inc.
6550 Rock Spring Drive, Suite 360
Bethesda, Maryland 20817

November 14, 1994

FOREWARD

The Department of Defense Intelligence Management System (DoDIMS) System Security Requirements document is being written as part of a generic set of accreditation documentation to support accreditation of DoDIMS at specific user sites. Each site will need to review this documentation and modify it, as necessary, to address specific site environment in which DoDIMS will operate.

Table of Contents

1.0 **Executive Summary**

The Department of Defense (DoD) Intelligence Management System (DoDIMS) is a software application designed to support the DoD and National intelligence communities in registering, validating, tracking and managing production requirements. It provides the mechanism for scheduling, deconflicting, tasking production and most importantly, provides the capability to track and manage overall production activities across operational and national planners and consumers. The DoDIMS program is structured under the definition of a DoD Intelligence Information Systems (DoDIIS) Core product. DoDIMS will operate in a system high mode at the Top Secret (TS), SCI Level.

DoDIMS will function as a client-server application using the Joint Deployable Intelligence Support System (JDISS) platform to host the DoDIMS application. Through a replication server process at each site DoDIMS will update other DoDIMS peer databases. Thus, a local site will have read/write capability of its respective data but read only capability of data at respective remote, peer sites. Eventually, a master, read-only DoDIMS database will be established at the Defense Intelligence Analysis Center. The Joint World-wide Intelligence Communications System (JWICS) will provide the network support for DoDIMS client-server communications. Use of JDISS, a current operational and accredited system, will allow connectivity with other intelligence systems required to support users during peacetime, crises, and wartime. The DoDIMS user will, therefore, have an integrated and interoperable tactical intelligence capability that includes host access, electronic mail, message handling, image processing, motion video processing and graphics capability.

This document summarizes the security requirements that DoDIMS must satisfy in order to be accredited as an operational system

2.0 **Background**

The functional requirements for DoDIMS are addressed in the Security Concept of Operations (SECONOPS). The SECONOPS addresses the basic system design and architecture, how DoDIMS is used, and provides a foundation document for the definition of the security requirements detailed in this document. Specific security test procedures used for accrediting DoDIMS will be developed in the DoDIMS Security Accreditation Test Plan and Security Accreditation Test Procedures, and will be based on the appropriate guidelines defined by this security requirements document.

3.0 **Purpose**

The DoDIMS Security Requirements document provides a vehicle for listing and establishing compliance with the minimum technical and non-technical requirements for automated information systems processing U.S. intelligence in a specific mode of operation.

4.0 **Mode of Operation**

DoDIMS will operate in the System High Mode at the TS/SI/TK level as defined in DCID 1/16, DDS-2600-5502-87, and the SECONOPS.

5.0 **Security Requirements**

5.1 **AIS Requirements.** The following tables provide the selection and compliance to administrative, environmental, and technical security requirements for DoDIMS which will operate in the System High Mode. The short description below provides a convenient reference to the requirements. Compliance to each requirement (by appropriate endorsement in column 3) implies adherence to the detailed description as provided in DoD 5200.28-STD, the "Orange Book" or DDS -2600-5502-87, respectively

Security Requirement	**Short Description**	**Compliance Verification**
1a. Conceptual Design	A systems engineering approach will be used to develop DoDIMS	Will comply
1b. Mode of Operation	System High as described in Paragraph 4.0	Will comply
1c. Identification of Accrediting Authority(ies)	Identify Accrediting Authorities	DIA/SY-1D
2. System Security Plan	The overall planning document suite of which this document is a part.	*Site will comply*

3. Appointment of an ISSO	An ISSO has been appointed for this AIS and will perform the documented duties. (An ISSO is required throughout the lifecycle.)	*Site will comply*
4. Access by Foreign Nationals	Foreign Nationals may not access DoDIMS except under strict conditions.	Foreign nationals will not be authorized access to DoDIMS.
5. Accreditation/ Reaccreditation	Accreditation documents must list specific modes of operations and other requirements.	*Site will comply*
6. Joint Accreditation	Applies when an AIS involves more than one accrediting authority.	*Site will comply, if applicable*
7. Interim Approval to Operate	Three conditions must be met if an interim approval is requested.	*Site will comply*
8. Security Briefings	All users, managers, and operators will be briefed on the need for sound security practices.	*Site will comply*
9. Automated Guard Processors	Automated guards or filters must satisfy certain criteria for proper filtering of data streams. They are interim measures and must meet specific accreditation assurances.	Not applicable

10. Protection of High Density/Transportable Storage Devices	Media containers will be marked with the highest sensitivity label until approved destruction or sanitization.	*Site will comply*
11. Memory Remanence	Memory will be safeguarded for the highest sensitivity of data ever recorded unless sanitized or destroyed.	Partial compliance by SUN operating system. *Site will comply* with written procedures for release of magnetic storage media.
12. Protected Software and Hardware	All hardware, software, firmware, etc. shall be protected to prevent disclosure, destruction, or modification.	Software control will be governed by the DoDIMS PMO. *Hardware control will be conducted by the site.*
13. Shipment of Equipment to High Risk Area	Systems for use in these areas must be protected from time of assembly until it is installed and operational. Areas are defined in "Department of State Composite Threat List" (issued quarterly).	Not applicable at this time.
14. Marking Storage Media	All removable media will bear external labels with the proper sensitivity labels and markings.	*Site will comply*
15. Marking of Printed Output	Comply with the appropriate paragraphs of the detailed description in the handbook for each of the four modes.	*Site will comply*

16. Manual Review of Human Readable Output	When markings cannot be trusted, properly cleared and authorized persons provide reliable human review of output media.	*Site will comply*
17. System Disposal Plan	A plan will be maintained for the secure disposal of the AIS, to include release, reutilization, or destruction of AIS components.	*Site will comply*
18. COMSEC	Communication links, data communications, and networks of AIS will be protected in accordance with COMSEC policies appropriate to the sensitivity level of data.	*Site will comply*
19. Use of Dial-up Lines	Dial-up use shall not be allowed for access to sensitive intelligence unless protections are certified or authorized by DIA.	Not applicable
20. TEMPEST	Processing facilities must be in compliance with the appropriate national policy on compromising emanations.	*Site will comply*
21. Physical Security	For sensitive intelligence, DIAM 50-3 standards shall apply. For SAPs, other appropriate standards apply.	*Site will comply*

22. Personnel Security	For each mode, specific clearance, access approvals, and need-to-know requirements must be met.	*Site will comply*
23. Commercial Vendor Maintenance	Maintenance personnel must be cleared and approved for access at the highest level of information on the system. Access will be given to only information/processes required to perform task. Uncleared personnel must be escorted by technically competent site personnel.	*Site will comply*
24. Technical Requirements for Dedicated Mode		Not Applicable

Paragraph numbers in the parentheses reference detailed descriptions of the requirements found in the Orange Book.

25. Technical Requirements for System High Mode	CY 2000 goal = C2 products based on Orange Book requirements CY 1992 Objective = automated controlled access protection for AISs at system high and above	
a. (2.2.1.1)	Discretionary Access Control (DAC)	Provided by operating system, DBMS, and application
b. (2.2.1.2)	Object Reuse	Provided by OS and *site procedures*

c. (2.2.2.1)	Identification and Authentication (I&A)	Provided by OS and application
d. (2.2.2.2)	Audit	Provided by OS and application
e. (2.2.3.1.1)	System Architecture	OS will comply
f. (2.2.3.1.2)	System Integrity	OS will comply
g. (2.2.3.2.1)	Security Testing	PMO will comply
h. (2.2.4.1)	Security Features User's Guide (SFUG)	Vendor documentation provides OS SFUG; PMO will provide DoDIMS SFUG.
i. (2.2.1.4)	Trusted Facility Manual (TFM)	Vendor documentation provides OS TFM; PMO will provide DoDIMS TFM.
j. (2.2.4.3)	Test Documentation	PMO will provide
k. (2.2.4.4)	Design Documentation	PMO will provide

The following (l through n) are additional requirements mandated by DCID 1/16:

l. Identification of User Terminals	OS will provide
m. Configuration Management	PMO will provide for software; JDISS PMO and *site will provide for hardware*
n. Trusted Distribution	PMO will provide
26. Technical Requirements for Compartmented Mode	Not Applicable

27. Technical Requirements for Multilevel Mode		Not Applicable
28. AUTODIN Connectivity		Not Applicable
29. DoDIIS Network Connectivity	AISs satisfying appropriate requirements for each of the four modes of operation, through the accreditation process, may be authorized connectivity to the DoDIIS Network when full DoDIIS Network Security for Information Exchange (DNSIX) capabilities are employed by the AIS, or its front end components. This is a CY 1993 requirement. Meeting the mandatory control requirement is a CY 1991 interim measure.	*Site will comply when appropriate and feasible*
30. Connectivity to other AISs and networks	For connection of AISs using other than separately accredited networks, specific requirements apply, including the need for both sensitivity markings and information markings for interconnections involving compartmented AISs.	*Site will comply when appropriate and feasible*
31.-32. Personal Computer Security Requirements		Not Applicable

33. System High and CMW Requirements	DIA Document DDS-2600-5502-87 describes what must be met for workstations to act as hosts in these modes.	*Site will comply when appropriate and feasible*.

5.2 **Separately Accredited Network.** *Site will comply when appropriate*.

5.3 **Due to Other Network Connections.** *Site will comply when appropriate*.

5.4 **Required by Data Originators.** Not applicable.

5.5 **From the Accrediting Authority.** Not applicable.

6.0 **Exceptions to Security Requirements.**

There are no exceptions to the security requirements.